STEVEN G. KALAR
Federal Public Defender
ELLEN V. LEONIDA
Assistant Federal Public Defender
555 - 12th Street, Suite 650
Oakland, CA 94607-3627
Telephone: (510) 637-3500
Fax: (510) 637-3507
Email: ellen_leonida@fd.org

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE TELEPHONE INFORMATION NEEDED FOR A CRIMINAL INVESTIGATION	CR 14-XR-90532 NC OPPOSITION TO GOVERNMENT'S APPLICATION, UNDER 18 U.S.C. § 2703(D), FOR CELL SITE LOCATION INFORMATION

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

DOCKETED CASES

FEDERAL STATUTES

OTHER FEDERAL AUTHORITIES

MISCELLANEOUS

INTRODUCTION

The Supreme Court recently, and aptly, noted that cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California*, 134 S. Ct. 2473, 2484 (2014). In addition to acting as cameras, phone books, maps, and computers, cell phones automatically generate a record of when and where they are used – effectively documenting the locations of all cell phone users, everywhere they go, every time of day.

Over the years, the government has obtained the location information of millions of cell phone users from their phone companies, without showing probable cause or obtaining a warrant. However, courts are increasingly recognizing that individuals have a reasonable expectation of privacy in "all [cell phones] contain and all they may reveal," *id.* at 2494, including what they reveal about the user's location. Under established Fourth Amendment principles, the government may not infringe upon these reasonable expectations of privacy unless it first obtains a warrant based on probable cause. Because the government here seeks access to cell site location information without obtaining a warrant or showing probable cause, the Court should deny its application.

BACKGROUND

Ninety percent of American adults have a cell phone.[1] Almost 40% of U.S. households have *only* cell phones.[2] As of December of 2013, there were 335.65 million wireless subscriber

[1] *Device Ownership Over Time*, Pew Research Internet Project, http://www.pewinternet.org/data-trend/mobile/device-ownership/ (last visited July 21, 2014).

[2] *Annual Wireless Industry Survey*, CTIA - The Wireless Association, http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey (last visited July 21, 2014).

accounts in the United States,[3] a number that exceeds the total population.[4] In 2013, American cell phone users generated 2.618 trillion minutes of calls and 1.91 trillion text messages.[5] According to a recent survey, nearly three quarters of adults with smartphones reported being within five feet of their phones most of the time.[6] Accordingly, people expect to be able to use their cell phones everywhere they go and, for the most part, they can.

Cell phones operate through the use of radio waves. Cellular service providers maintain a network of radio base stations (also called cell sites or cell towers) throughout their coverage areas. *Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance, Hearing before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations, of the H. Comm. on the Judiciary*, 113th Cong., 50 (2013) (written testimony of Prof. Matt Blaze, University of Pennsylvania) [hereinafter 2013 ECPA Hearing]. A base station consists of multiple antennas facing in different directions. Typically, there are three antennas, each covering a 120-degree arc, resulting in three pie-shaped sectors. Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, U.S. Att'y Bull., Nov. 2011, at 19-20.

Cell phones periodically identify themselves to the closest base station (the one with the strongest radio signal) as they move throughout the coverage area. 2013 ECPA Hearing at 50 (Blaze testimony). Whenever a cell phone user makes or receives a call or text message, his phone connects, via radio waves, to an antenna on a cell site, generating cell site location

---

[3] *Annual Wireless Industry Survey*, CTIA - The Wireless Association, http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey (last visited July 21, 2014).

[4] *U.S. and World Population Clock*, U.S. Census Bureau, http://www.census.gov/popclock/ (last visited July 21, 2014) (When visited on July 21, population listed at 318.49 million.)

[5] *Annual Wireless Industry Survey*, *supra* note 2.

[6] Harris Interactive, *2013 Mobile Consumer Habits Study*, Jumio, Inc., 2 (June 2013), http://pages.jumio.com/rs/jumio/images/Jumio%20-%20Mobile%20Consumer%20Habits%20Study-2.pdf

information ["CSLI"]. If a cell phone moves away from the base station with which it started a call and closer to another base station, it connects seamlessly to the next base station. *Id.*

As the number of cell phones has increased, the number of cell sites has had to increase as well:

> A sector can handle only a limited number of simultaneous call connections given the amount of radio spectrum 'bandwidth' allocated to the wireless carrier. As the density of cellular users grows in a given area, the only way for a carrier to accommodate more customers is to divide the coverage area into smaller and smaller sectors, each served by its own base station and antenna. New services, such as 3G and LTE/4G Internet create additional pressure on the available spectrum bandwith, usually requiring, again, that the area covered by each sector be made smaller and smaller.

Id. at 54. Densely populated urban areas therefore have more towers covering smaller sectors. Within one mile of the San Francisco Federal Courthouse, for example, there are 71 towers and 781 separate antennas.[7]

The trend is toward smaller and smaller base stations, called microcells, picocells, or femtocells, which cover a very specific area, such as one floor of a building, the waiting room of an office, or a single home. *Id.* at 43-44. The effect of this proliferation of base stations is that "knowing the identity of the base station (or sector ID) that handled a call is tantamount to knowing a phone's location to within a relatively small geographic area … sometimes effectively identifying individual floors and rooms within buildings." *Id.* at 55-56. Although the ability of cell providers to track a phone's location within a sector varies based on a number of factors, it is increasingly possible to use CSLI to "calculate users' locations with a precision that approaches that of GPS." *Id.* at 53.

[7] Information regarding the concentration of towers in a given geographic area can be found on a public database, available at http://www.antennasearch.com/sitestart.asp

Tools and techniques are constantly being developed to track CSLI with ever-greater precision. Providers can currently triangulate the location of a phone within a sector by correlating the time and angle at which it connects with multiple base stations. *Id.* at 56. Providers also are developing technologies that will track CSLI whenever a phone is turned on, whether or not it is in use. *Id.* at 57. Because this information costs little to collect and store, providers tend to keep it indefinitely. *Electronic Communications Privacy Act Reform and the Revolution in Location Based Technologies and Services, Hearing before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong., 16 (2010) (testimony of Prof. Matt Blaze) [hereinafter 2010 ECPA Hearing].

The ability to track people through their cell phones is, obviously, very appealing to law enforcement. *See* O'Malley, *supra*, at 26 (noting that provider records "contain accurate date, time, and location information" and "unlike a witness' memory, are not prone to impeachment based on their accuracy, reliability, or bias"); 2013 ECPA Hearing at 61 ("These characteristics – ubiquitous and continuous availability, lack of alerting, and high precision – make network-based cellular tracking an extremely attractive and powerful tool for law enforcement surveillance.").

Consequently, each year the United States government seeks CSLI for tens of thousands of people. 2010 ECPA Hearing at 80 (written testimony of United States Magistrate Judge Stephen Wm. Smith). The government almost always seeks this information by way of sealed applications and orders. *Id.* at 87. In this district alone, the Office of the United States Attorney has identified 760 matters in its case management system that were likely to involve applications for location-tracking information between January 1, 2008, and January 3, 2013. Declaration of Patricia J. Kenney in Support of the Department of Justice's Motion for Summary Judgment as to Part 1 of Plaintiff's Freedom of Information Act Request at 10, *American Civil Liberties Union of Northern California v. Department of Justice*, No. 12-cv-4008 MEJ (N.D. Cal. Sept. 23, 2013).

DISCUSSION

I. THE FOURTH AMENDMENT PROHIBITS WARRANTLESS SEARCH AND SEIZURE OF CSLI

A. CSLI Is Protected by the Fourth Amendment Right to Privacy

The Fourth Amendment prohibits the government from collecting an individual's historical location tracking information without a warrant. Since at least 1967, the Supreme Court has recognized that the Fourth Amendment protects an individual's right to privacy, even in public places. *Katz v. United States*, 389 U.S. 347, 351 (1967). *Katz* held that when the government infringes upon a subjective expectation of privacy that society recognizes as reasonable, it effects a search and seizure within the meaning of the Fourth Amendment. *Id.* at 353. Thus, in *Katz*, the government was found to have violated the defendant's Fourth Amendment rights by eavesdropping on his private conversation in a public phone booth. *Id.*

In *United States v. Knotts*, the Court first applied the *Katz* test to electronic surveillance, holding that the Fourth Amendment was not violated when the government used a beeper to track a car from one location to another. 460 U.S. 276, 277 (1983). The beeper tracking in *Knotts* did not implicate the Fourth Amendment because "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *Id.* at 281. However, the Court left open the possibility that advances in surveillance technology would require a reevaluation of its decision. *Id.* at 283-84.

The following year, in *United States v. Karo*, the Court limited *Knotts* to electronic surveillance *in public places*. 468 U.S. 705, 714 (1984). In *Karo*, the police placed a beeper in a container belonging to the defendant and monitored its location electronically, including while it was inside a private residence. *Id.* at 708-10. The Court held that the continued monitoring of the beeper inside the home was an unconstitutional trespass into the residence by electronic

means – even though the officers could not have known, when they planted the tracking device, that it would end up inside a house. *Id.* at 715; *see also Kyllo v. United States*, 533 U.S. 27, 34 (2001) (holding that the government engages in a search in violation of the Fourth Amendment by using a thermal imager to detect heat signatures inside a house that would be invisible to the naked eye).

More recently, in *United States v. Jones*, five Justices concluded that prolonged, electronic location monitoring by the government impinges upon a legitimate expectation of privacy in violation of the Fourth Amendment. 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring); *id.* at 965 (Alito, J., concurring). In *Jones*, the government placed a GPS tracker on the defendant's car and used it to monitor the car's location – on public thoroughfares – for 28 days. *Id.* at 948. The majority opinion held that the government had violated the Fourth Amendment by the physical trespass of placing the tracker on the vehicle, and it therefore did not need to address whether the location tracking violated a reasonable expectation of privacy. *Id.* at 949. It explicitly noted, however, that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." *Id.* at 953 (emphasis in original).

The five Justices who did engage in a *Katz* analysis concluded that the government's actions in tracking the car's location violated the Fourth Amendment. *Id.* at 964 (Alito, J., concurring); *id.* at 955 (Sotomayor, J., concurring).[8] Despite the fact that the government tracked the car only as it travelled in plain sight on public streets and highways, Justice Alito concluded that the GPS monitoring "involved a degree of intrusion that a reasonable person would not have

[8] Justice Sotomayor, while agreeing with Justices Alito, Ginsburg, Breyer, and Kagan that an analysis under *Katz* was appropriate, nonetheless wrote separately because she also joined the majority in concluding that the physical trespass of placing the tracker on the car was an independent Fourth Amendment violation. *Jones*, 132 S. Ct. at 954-55 (Sotomayor, J., concurring).

anticipated." *Id.* at 964 (Alito, J., concurring). Consequently, he found that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id.* Notably, this conclusion did not depend upon on the type of technology used to track the car in *Jones*; rather, Justice Alito discussed the proliferation of modern devices that track people's movements, noting that cell phones were "perhaps [the] most significant" among these. *Jones*, 132 S. Ct. at 963 (Alito, J., concurring).

Justice Sotomayor agreed that prolonged electronic surveillance violates the Fourth Amendment. *Id.* at 955 (Sotomayor, J., concurring). She added, however, that "even short-term monitoring" raises concerns under *Katz* because "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* When governmental actions intrude upon someone's privacy to that degree, a warrant is required. *Id.*

Here, as in *Jones*, the government seeks permission to track individuals, without a warrant, over an extended period of time, by electronic means.[9] CSLI, like GPS, provides the government with a comprehensive, intimate portrait of an individual's life. Most people would not expect that the government can access, without a warrant, records tracking their movements for weeks or months at a time – and that expectation is a reasonable one.

The ability of CSLI to track people inside buildings raises additional Fourth Amendment concerns. *Kyllo* and *Karo* prohibit warrantless intrusions into the home, intended or not, by means of technology. *Kyllo*, 533 U.S. at 34; *Karo*, 468 U.S. at 17. As the Court acknowledged in *Kyllo*, "the rule we adopt must take account of more sophisticated systems that are already in use or in development." *Kyllo*, 533 U.S. at 36. Because CSLI is generated by radio waves, it

[9] This Opposition addresses CSLI in general terms only, because no information was disclosed about the type of location information the government is seeking or the length of time covered by its application.

inevitably collects information from inside buildings, including private homes. Especially as cell sites cover smaller and smaller sectors, cell site location tracking to (or even within) a specific home is inevitable. Even today, the government has no way of restricting its requests for CSLI to public spaces – which is one reason that governmental requests for this information should be supported by probable cause and a warrant.

B. This Court Should Follow the Eleventh Circuit in Holding That Historical Cell Site Location Information Is Protected by the Fourth Amendment

As noted above, the data the government seeks when it requests CSLI is much more comprehensive, and much more apt to reveal intimate information, than the location of someone's car. Accordingly, the Eleventh Circuit recently held that, in light of the *Jones* concurrences, government requests for CSLI are subject to the warrant requirement of the Fourth Amendment. *United States v. Davis*, ___ F.3d ___, 2014 WL 2599917 at *10 (11th Cir. 2014). *Davis* compared the information revealed to the government via a GPS device on a vehicle with that revealed by CSLI and found that the violation of privacy rights implicated by disclosure of CSLI was much more significant:

> One's car, when it is not garaged in a private place, is visible to the public, and it is only the aggregation of many instances of the public seeing it that make it particularly invasive of privacy to secure GPS evidence of its location…In contrast, even on a person's first visit to a gynecologist, a psychiatrist, a bookie, or a priest, one may assume that the visit is private if it was not conducted in a public way. One's cell phone, unlike an automobile, can accompany its owner anywhere. Thus, the exposure of the cell site location information can convert what would otherwise be a private event into a public one. When one's whereabouts are not public, then one may have a reasonable expectation of privacy in those whereabouts.

Id. at *8. Because the location of a cell phone is so apt to reveal private information about its owner, *Davis* concluded, "even one point of cell site location data can be within a reasonable expectation of privacy." *Id.* Indeed, while people are in their cars only while travelling from one

place to another, most Americans are within five feet of their phones most of the time.[10] Especially in urban settings, where cell towers are more plentiful, this means that a cell phone – and, by extension, its owner – can be tracked with disquieting precision.[11]

The government urges this Court to disregard *Davis* and instead follow the Third and Fifth Circuits in holding that the government need not procure a warrant before acquiring CSLI. *See In re Application*, 724 F.3d 600 (5th Cir. 2013); *In the Matter of the Application*, 620 F.3d 304 (3d Cir. 2010). The Third Circuit opinion, which was issued before *Jones* was decided, is based on the proposition that location monitoring does not implicate Fourth Amendment privacy rights.[12] *In the Matter of the Application*, 620 F.3d at 313 ("The *Knotts/Karo* opinions make clear that the privacy interests at issue are confined to the interior of the home."). This reasoning cannot stand in the face of *Jones*, which explains that the government's prolonged surveillance of individuals, even in public places, *does* implicate the Fourth Amendment. *Jones*, 132 S. Ct. at 953; *id.* at 955 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring).

The Fifth Circuit, on the other hand, held that any disclosure of private information to a third party destroys all privacy interests in the information; *i.e.*, because the cell phone provider collects the CSLI data, the subscriber cannot claim a legitimate interest in its privacy. *In re Application*, 724 F.3d at 610-11. To reach this conclusion, the Fifth Circuit posits that it is

---

[10] Harris Interactive, *2013 Mobile Consumer Habits Study*, Jumio, Inc., 2 (June 2013), http://pages.jumio.com/rs/jumio/images/Jumio%20-%20Mobile%20Consumer%20Habits%20Study-2.pdf

[11] Even cases that disagree on the constitutionality of warrantless CSLI tracking acknowledge that the tracking is precise. *See In re Application*, 724 F.3d 600, 609 (5th Cir. 2013) ("The reason that the Government seeks such information is to locate or track a suspect in a criminal investigation. The data must be precise enough to be useful to the government… it can narrow someone's location to a fairly small area."); *see also* 2013 ECPA Hearing at 61 ("The increasingly high resolution that the cell site tracking can achieve in densely populated areas – and the ability to provide this data even when the handset is indoors – can paint an even richer picture of an individual's movements than can vehicle-based GPS devices.").

reasonable – and constitutional – to force people to choose between preserving their Fourth Amendment rights and owning a cell phone. *Id.* at 613. As discussed in section II, below, the Supreme Court has never taken such an extreme position. Moreover, the Court's recent decision in *Riley v. California* affirms that the protections of the Fourth Amendment extend to information generated by our cell phones even when it is shared with the provider. 134 S. Ct. 2473 (2014).

C. *Riley v. California* Implicitly Recognizes a Privacy Interest in CSLI

After *Riley*, there can be no doubt that individuals have a reasonable expectation of privacy in cell phone location data. In a rare, unanimous Fourth Amendment decision, the Court explained that cell phones "hold for many Americans the privacies of life." *Id.* at 2495 (citation and internal quotation marks omitted). *Riley*'s focus on the wealth of information revealed by an individual's cell phone, and the attendant right to privacy in that information, applies beyond the limited context of searches incident to arrest.[13]

Because cell phones have the capacity to expose such vast amounts of personal information about their owners, the Court refused to engage in a "mechanical application" of precedent. *Id.* at 2484. *Riley* thus rejected the government's efforts to analogize cell phone information to any pre-digital counterpart. *See id.* at 2488 ("The United States asserts that a

---

[12] As discussed in section V, infra, the Third Circuit did hold that 18 U.S.C. § 2703 gives magistrates the discretion to require a warrant for CSLI on a case-by-case basis. *In the Matter of the Application*, 620 F.3d at 319.

[13] Commentators agree that *Riley*'s holding extends well beyond the particular warrant exception at issue. Legal scholars have widely characterized the holding as sweeping, and one that will have broad implications in other areas. *See, e.g.*, Marc Rotenberg & Alan Butler, *Symposium: In* Riley v. California, *A Unanimous Supreme Court Sets Out Fourth Amendment for Digital Age*, SCOTUSblog (June 26, 2014, 6:07 PM), http://www.scotusblog.com/2014/06/symposium-in-riley-v-california-a-unanimous-supreme-court-sets-out-fourth-amendment-for-digital-age/ ("The Court's conclusion that *data is different* will affect not only digital search cases, but also the NSA's bulk record collection program, access to cloud-based data, and the third-party doctrine."); Adam Liptak, *Major Ruling Shields Privacy of Cellphones*, N.Y. Times (June 25, 2014), http://www.nytimes.com/2014/06/26/us/supreme-court-cellphones-search-privacy.html ("While the decision will offer protection to the 12 million people arrested every year, many

search of all data stored on a cell phone is 'materially indistinguishable' from searches of these sorts of physical items. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together."). The Court declared, without qualification, that "[m]odern cell phones, *as a category*, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." *Id.* at 2488-89 (emphasis added).

Historical location data generated by cell phones served as one of the Court's chief examples of "the privacies of life" that cell phone metadata exposes. *See id.* at 2490 ("Data on a cell phone can also reveal where a person has been. Historic location information… can reconstruct someone's specific movements down to the minute, not only around town, but within a particular building."). The Court cited with approval Justice Sotomayor's concurrence in *Jones*, in which she concluded that generating and monitoring "a precise, comprehensive record of a person's public movements" infringes upon a reasonable expectation of privacy that is protected by the Fourth Amendment. *Id.* at 2490 (citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)).

Riley also contains echoes of the "mosaic theory" of privacy adopted by Justices Sotomayor and Alito in their *Jones* concurrences, noting that "[a] cell phone collects in one place many distinct types of information… that reveal much more in combination than any isolated record." *Id.* at 2489.[14] The Court explained that aggregating, then analyzing, this data intrudes upon a protected privacy interest: "The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet." *Id; see also Davis*, ___ F.3d

---

for minor crimes, its impact will most likely be much broader.").

___, 2014 WL 2599917 at *6 (noting that the government often relies on mosaic theory to establish that aggregated data is far more revealing than the sum of its parts).

Riley thus stands in direct opposition to the government's position in this case. Cell phones, as the *Riley* court acknowledged, are ubiquitous. *See* 134 S. Ct. at 2490 ("According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower."). The data they collect is "qualitatively different" than that contained in other objects, for purposes of Fourth Amendment analysis. *Id.* *Riley's* discussion of the nature of cell phones and our dependence upon them forecloses any argument that it is "reasonable" to expect that the 90% of American adults who carry cell phones thereby waive their Fourth Amendment right to not be subject to constant government surveillance.

II. CELL PHONE SUBSCRIBERS DO NOT FORFEIT THEIR FOURTH AMENDMENT RIGHTS SIMPLY BECAUSE THEIR CSLI RECORDS ARE MAINTAINED BY THIRD-PARTY CELL PHONE COMPANIES

A. An Individual Does Not Lose the Right to Privacy in CSLI Simply Because It Is Disclosed to a Cell Phone Provider

The government urges this Court to follow the Fifth Circuit by analogizing the CSLI at issue here to the bank records and pen registers at issue in *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976). *Smith* and *Miller* held that, by voluntarily sharing dialed numbers with the phone company and banking records with the bank, the consumer waived any right to privacy in those records for purposes of the Fourth Amendment. *Smith*, 442 U.S. at 742; *Miller*, 425 U.S. at 442-43. The fact that the cell phone providers maintain records of individuals' CSLI does not, however, diminish the individuals' privacy interest in those records. Exposing information to a third party does not necessarily

[14] *See also, e.g., United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010) (adopting, in lower court

waive one's expectation of privacy and attendant Fourth Amendment protections.[15]

The third-party doctrine discussed in *Smith* and *Miller* is inapplicable to an era where people routinely and unthinkingly disclose the most intimate details of their lives to their cell phone providers. As Justice Sotomayor recognized in *Jones*, our increasing dependence on technology in daily life requires a re-evaluation of the question of "privacy" in the context of the Fourth Amendment:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *E.g., Smith,* 442 U.S., at 742, 99 S. Ct. 2577; *United States v. Miller,* 425 U.S. 435, 443, 96 S. Ct. 1619, 48 L. Ed. 2d 71 (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.

132 S. Ct. at 957 (Sotomayor, J., concurring); *see also* Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is That What* Katz *Is Made Of?*, 41 U.C. Davis L. Rev. 781 (2008) (arguing that the third-party doctrine is "extremely dangerous in an increasingly technological world" and must be reconsidered in light of actual societal expectations of privacy in digital information).

The Supreme Court has consistently revisited its Fourth Amendment jurisprudence in

---

opinion in *Jones*, the "mosaic" theory to hold that GPS tracking of a car is a "search").

[15] *See Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (holding that patients have reasonable expectation of privacy in results of medical tests, despite their voluntary disclosure of those results to hospital personnel); *Bond v. United States*, 529 U.S. 334, 338-39 (2000) (holding that traveler retains reasonable expectation of privacy in bag placed in overhead bin of a bus, despite knowledge that other passengers can handle and move bag); *Quon v. Arch Wireless Operating Co. Inc.*, 529 F.3d 892, 905-07 (9th Cir. 2008) (holding that police officer had reasonable expectation of privacy in contents of text messages sent on phone owned by police department despite fact that third-party server had access to the messages *and* despite department policy stating there was no expectation of privacy in texts), *rev'd on other grounds*, 560 U.S. 746 (2010)); *United States v. Taketa*, 923 F.2d 665, 677 (9th Cir. 1991) (holding that agent had reasonable expectation of privacy in not being secretly videotaped in someone else's office).

light of evolving technology. *See Kyllo*, 533 U.S. at 33-34 ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."). *Jones* thus recognized that GPS technology was qualitatively different than its physical surveillance counterpart.[16] 132 S. Ct. at 954. *Riley* similarly rejected any comparison between physical items in an arrestee's possession and his cell phone. *See* 134 S. Ct. at 2485 ("A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in [*United States v. Robinson*, 414 U.S. 218 (1973)]").

Here, as in *Jones* and *Riley*, the realities of modern technology preclude the mechanical application of 35-year-old precedent. In 1979, the year *Smith* was decided, Jimmy Carter was president, *The Dukes of Hazard* premiered on CBS, and telephones travelled only as far as their cords would allow. The Court could not have foreseen that one day the telephone company would be automatically electronically tracking the vast majority of Americans everywhere, all the time, and regularly turning that information over to the government. It is inconceivable that *Smith* and *Miller* intended so far-reaching an abrogation of our Fourth Amendment rights.[17]

The advent of technologies that enable more intrusive police surveillance cannot be permitted to "erode the privacy guaranteed by the Fourth Amendment." *See Kyllo*, 533 U.S. at

---

[16] Even the *Knotts* court acknowledged that its analysis was subject to change with evolving surveillance technology. 460 U.S. at 283-84 ("If such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."); *see also United States v. Pineda-Moreno*, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, J., dissenting) ("When requests for cell phone location information have become so numerous that the telephone company must develop a self-service website so that law enforcement agents can retrieve user data from the comfort of their desks, we can safely say that 'such dragnet-type law enforcement practices' are already in use.").

[17] Indeed, although the government's concession in *Riley* that a search had occurred enabled the Court to avoid fully reconsidering *Smith*, the Court took the opportunity to explain that the pen register in *Smith* bore little relationship to the phone data being mined by the government. *Riley*, 134 S. Ct. at 2492. The Court noted that, even on an old-fashioned flip phone, a cell phone's call log (and thus its metadata) "contained more than just phone numbers," including substantial personal identifiers, rendering a case about pen registers of little utility in deciding the Fourth Amendment question in the context of cell phones. *Id.* at 2493.

34. This Court should join others across the country in rejecting "the fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by 'choosing' to carry a cell phone." *In the Matter of an Application*, 809 F. Supp. 2d 113, 127 (E.D. N.Y. 2011); *see also In the Matter of an Application*, 736 F. Supp. 2d 578, 596 (E.D. N.Y. 2010) ("The Fourth Amendment cannot properly be read to impose on our populace the dilemma of either ceding to the state any meaningful claim to personal privacy or effectively withdrawing from a technologically maturing society."); *cf. In re United States*, 2006 WL 1876847 at **1, 3 (N.D. Ind. 2006) (unpublished) (denying government's appeal from magistrate's order denying prospective and historical CSLI without a warrant); *cf. also In Matter of United States*, ___ F. Supp. 2d ___, 2014 WL 1395082 at *1 (D. D.C. 2014) (noting "serious statutory and constitutional questions" raised by government's application for historical CSLI and ordering amicus and the government to submit "evidence and substantive briefing" before deciding "whether this application should be granted in its current form -- and without a showing of probable cause").

B. CSLI Is Not Voluntarily Conveyed to a Third Party

Even under the third-party doctrine articulated in *Smith* and *Miller*, however, cell phone users would retain a constitutionally protected privacy interest in their CSLI. *Smith* held that there was no privacy interest in dialed numbers because the person using the telephone intentionally conveyed the number to the telephone company for the express purpose of having the carrier connect him to that number. 442 U.S. at 742. The consumer also received a list of numbers dialed on his monthly bill, confirming that the phone company was recording this information. *Id.* Similarly, *Miller* declined to extend Fourth Amendment protection to bank documents (*e.g.*, checks, deposit slips) because these documents were intentionally shared by the consumer with bank employees in order to achieve the consumer's purpose (*e.g.*, transferring

money to another entity, depositing money in an account) and the bank was a party to these transactions. 425 U.S. at 440-43.

CSLI, on the other hand, is not knowingly and intentionally conveyed by the consumer to anyone but rather generated automatically by radio waves. People do not use their cell phones as tracking devices or expect that the government will do so. In contract to *Smith*-era telephone bills, which listed toll calls, cell phone users do not receive a report of their CSLI from their service providers. Nor do providers inform them how long they retain CSLI. Cell phone users do not affirmatively convey CSLI, nor can they control its disclosure. Accordingly, the Third and Eleventh circuits have rejected the argument that CSLI is voluntarily conveyed by cell phone users. *Davis*, ___ F.3d ___, 2014 WL 2599917 at *9; *In the Matter of the Application*, 620 F.3d at 317.

The Ninth Circuit also has rejected the general theory that passive transmission of data to a third party waives a consumer's Fourth Amendment rights. In *United States v. Forrester*, the court held that email and IP addresses were not protected by the Fourth Amendment. 512 F.3d 500, 510 (9th Cir. 2008). Significantly, the court drew a distinction between this information, which the consumer conveys intentionally for purposes of delivering his email or directing his browser to a specific address, and data that is "merely passively conveyed through third party equipment." *Id.* The court thus retained Fourth Amendment protection for information that is not conveyed voluntarily to achieve a purpose of the consumer. *Id.* at 511 ("E-mail, like physical mail, has an outside address 'visible' to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient.").

Even the *Smith* Court recognized that the voluntary disclosure of information to a third

party does not erase all Fourth Amendment protection.[18] 442 U.S. at 739-40. *Smith* distinguished between records of dialed telephone numbers and the content of telephone conversations, which it acknowledged remained protected by the Fourth Amendment. *Id.* The location information at issue here is more analogous to the content of a communication than to an address. Tracking a person via the location of his cell phone is akin to electronically following him everywhere he goes, inside and outside, day and night, for the period of surveillance. This is far more intrusive than recording the phone numbers he dials, and it warrants greater Fourth Amendment protection. *See Davis*, ___ F.3d ___, 2014 WL 2599917 at *8 ("cell site data is more like communications data than it is like GPS information. That is, it is private in nature rather than being public data that warrants privacy protection only when its collection creates a sufficient mosaic to expose that which would otherwise be private.").

III. CSLI IS NOT A BUSINESS RECORD OF THE PROVIDER

A. A Service Provider's Ability to Access CSLI Does Not Defeat the Subscriber's Reasonable Expectation of Privacy

Relying on the Fifth Circuit's decision, the government argues that it may obtain CSLI because "a historical cell site record 'is clearly a business record' of the cell phone provider," Gov't Application at 5 (quoting *In the Matter of the Application*, 724 F.3d at 612), and, as such, may be obtained by subpoena or similar compulsory process. The government contends that it need not, therefore, establish probable cause before acquiring CSLI and is subject only to the Fourth Amendment's "reasonableness standard for compulsory process." *Id.*

The fundamental flaw in this argument is that it begs the critical question of whether cell

[18] Even if disclosure to a third party diminishes an individual's privacy interest, *Riley* explicitly held that "diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely." 134 S. Ct. at 2488. "To the contrary, when 'privacy-related concerns are weighty enough' a 'search may require a warrant notwithstanding the diminished expectations of privacy.'" *Id.* (quoting *Maryland v. King*, 133 S. Ct. 1958, 1979 (2013)).

phone users have a reasonable expectation of privacy in their location information. *See Smith*, 442 U.S. at 742 ("petitioner's argument that [the pen register] installation and use constituted a 'search' necessarily rests upon a claim that he had a 'legitimate expectation of privacy' regarding the numbers he dialed on his phone"); *Miller*, 425 U.S. at 442 ("We must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents."). If a reasonable expectation of privacy exists, the fact that the record is maintained in the course of business does not strip it of Fourth Amendment protection.

As discussed above, cell phone users do have a reasonable expectation of privacy in their CSLI. Therefore, the government cannot obtain it simply by issuing a subpoena. *See Miller*, 425 U.S. at 444 ("[T]he general rule that the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant" applies only when "no Fourth Amendment interests… are implicated.").

A second flaw in the government's argument is that, as discussed above, cell phone users do not knowingly and voluntarily convey their location information to the cell phone provider. The voluntariness question is significant in the business records analysis. *See Smith*, 442 U.S. at 445 (stating that it does not matter "whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed" but rather whether "petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record"). Two of the three circuits that have addressed whether cell phone users voluntarily share their location information have concluded that they do not. *See Davis*, ___ F.3d ___, 2014 WL 2599917 at *9 (following Third Circuit in rejecting argument that cell phone users knowingly and voluntarily share with providers their historical CSLI); *In the Matter of the Application*, 620 F.3d at 317 ("A cell phone customer has not 'voluntarily' shared his location information with a

cell provider in any meaningful way.").[19]

Once a subscriber has demonstrated a reasonable expectation of privacy in records held by a third party, the question becomes whether the disclosure or some other factor defeats the Fourth Amendment protection otherwise accorded to the records. In *United States v. Warshak*, the Sixth Circuit rejected the argument that an internet service provider's ability and right to access the contents of a subscriber's emails eliminated the subscriber's reasonable expectation of privacy in his emails. 631 F.3d 266, 286-87 (6th Cir. 2010). The ISP's control over and ability to access the emails "will not be enough to overcome an expectation of privacy." *Id.* at 287 (internal quotation marks omitted). There is no reason the Court should reach a different conclusion in this case.

B. Service Providers Were Forced by the Government to Configure Their Networks to Generate CSLI for Law Enforcement Purposes

Moreover, CSLI is not a business record of the provider because the government requires cell phone companies to record CSLI for law enforcement purposes and to give law enforcement access to it. In 1994, Congress enacted the Communications Assistance for Law Enforcement Act ["CALEA"], 18 U.S.C. §§ 1001-1010, which required all cell phone service providers to build into their networks equipment capable of "expeditiously isolating and enabling the government… to access call-identifying information." 47 U.S.C. § 1002(a). "Call-identifying information" includes CSLI. *U.S. Telecomm. Ass'n v. FCC*, 227 F.3d 450, 453 (D.C. Cir. 2000).

CALEA was enacted for the express purpose of allowing law enforcement "to intercept communications involving advanced technologies such as digital or wireless transmission

[19] Other cases that the government cites to support this claim also fail to advance its argument. In *Donaldson v. United States*, 400 U.S. 517 (1971), and *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735 (1984), the Court found no reasonable expectation of privacy because people had intentionally disclosed the information at issue to someone else. Similarly, in *United States v. Golden Valley Elec. Ass'n*, the

modes." H.R. Rep. No. 103-827(I) at 9 (1994); *see also* Communications Assistance For Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (enacting CALEA "to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes"). Following the enactment of CALEA, the Telecommunications Industry Association, after extensive negotiations with the FBI, promulgated technical standards outlining the "technical features, specifications, and protocols" a network must incorporate to comply with CALEA. *U.S. Telecomm. Ass'n*, 227 F.3d at 455. These standards are known as the "J-Standard." *Id.* Providers who do not comply with these standards are subject to fines of $10,000.00 per day. *Id.* at 455.

When the J-Standard first was adopted by the FCC, telecommunications industry associations, along with privacy rights groups, challenged it on the grounds that CSLI was outside the scope of CALEA. *Id.* at 455. They objected that the requirement that their networks track and provide CSLI "effectively converts ordinary mobile telephones into personal location-tracking devices, giving law enforcement agencies access to far more information than they previously had." *Id.* at 455-56. The FCC disagreed, and the courts ultimately ruled that CSLI is "call-identifying information" under CALEA and that the providers are, therefore, required to collect it and to make it available to law enforcement. *Id.* at 463.

Today, the J-Standard dictates the default network architecture of every cell phone service provider in the United States. *See* Micah Sherr, et al., *Can They Hear Me Now? A Security Analysis of Law Enforcement Wiretaps*, Proc. 16th ACM Conf on Computer & Comms. Sec. 512, 514 (Nov. 2009) ("This architecture is the only currently fielded standard for complying with CALEA."). It mandates that every cell network include elements that function as "interception

---

reasonableness standard applied because the records at issue were ones in which the consumer had no reasonable expectation of privacy. 689 F.3d 1108, 1116—17 (9th Cir. 2012).

access points" that have the ability to convey CSLI to law enforcement. *Id.* at 514-15. Consequently, cell phone users have no choice but to obtain their cell phone service from a company that is required, by the federal government, to track their CSLI and to make it available to law enforcement.

In light of this history, the government's claim that "[c]ell phone providers maintain cell site information for their own purposes, including billing and advertising, and not because the government mandates the compilation of such information; no federal law requires a company to create or keep historical cell site records," Govt. Letter Brief, at 1, is disingenuous, at best. Indeed, when engaged in litigation to force cell phone providers to create networks capable of transmitting CSLI to law enforcement, the Justice Department recognized the privacy interest at stake and conceded, in its brief in *U.S. Telecomm. Ass'n*, that "a pen register order does not by itself provide law enforcement with authority to obtain location information, and we have never contended otherwise." 227 F.3d at 464. The government cannot now claim that CSLI is information that cell phone service providers independently choose to record and preserve that coincidentally happens to be useful to law enforcement.

IV. THE STORED COMMUNICATIONS ACT DID NOT CONTEMPLATE CSLI

The government also argues that Congress determined that it could obtain CSLI based on only a court order, without showing probable cause, when it enacted the Stored Communications Act ["SCA"], including 18 U.S.C. § 2703(d).[20] Because CSLI is protected by the Fourth Amendment, as discussed above, a warrant supported by probable cause is required, and the government may not obtain CSLI based on a lesser showing, even if it complies with the statute. *See Davis*, ___ F.3d ___, WL 2599917 at *3 (holding that "[t]he obtaining of [cell site location]

data without a warrant is a Fourth Amendment violation" even though government obtained information under a § 2703(d) order). "It is clear, of course, that no Act of Congress can authorize a violation of the Constitution." *Almeida-Sanchez v. United States*, 413 U.S. 266, 272 (1973).

Moreover, there is no indication in the SCA or the relevant legislative history that Congress considered, or intended to address, CSLI in promulgating the SCA. *See In re United States*, 441 F. Supp. 2d 816, 833 (S.D. Tex. 2006) ("Hybrid proponents concede that the SCA was not specifically enacted as the mechanism to collect cell site data."). The legislative history of the SCA establishes that Congress enacted it primarily to "'protect against the unauthorized interception of electronic communications.'" *In the Matter of the Application*, 620 F.3d at 313 (quoting S. Rep. No. 99-541, at 1 (1986)). Although the legislative history refers to cell phones, it discusses location information only with respect to "tracking devices" or transponders, which it defines as "one-way radio communication devices that emit a signal on a specific radio frequency" – not cell phones. S. Rep. No. 99-541 at, *e.g.*, 2, 4, 9, 10. The section describing "cellular telephones" does not mention location information. *Id.* at *9.

The SCA was last amended in 1994, by CALEA. That amendment addressed CSLI only by precluding the government from obtaining it based solely on a pen register application. *In the Matter of the Application*, 620 F.3d at 315 n.1 (quoting 47 U.S.C. § 1002(a)(2)(B)); *see also* 2010 ECPA Hearing at 2 (2010) (Rep. Sensenbrenner: "In enacting . . . CALEA, Congress specifically instructed that a person's location information cannot be acquired solely pursuant to a pen register."). In fact, Congress held a series of hearings in 2010 to address CSLI precisely because it had not considered the subject when it enacted or amended the SCA. *See* 2010 ECPA

[20] *See* Govt. Letter Brief at 7 ("In the Stored Communications Act, including § 2703(d), Congress has enacted legislation controlling government access to historical records of cell-phone providers. When

Hearing at 2 (Rep. Sensenbrenner: "Considering that the ECPA was enacted in 1986, well before the proliferation of cell phones and other technologies, I think it is fair to say that the statute does not speak specifically to these issues."); *id.* at 82 (Magistrate Smith: "ECPA does not explicitly refer to 'cell site' or other location information from a cell phone.").

A review of the explosive growth in cell site networks and the proliferation of cell phones over the past 28 years further belies any claim that the 1986 SCA adequately protects cell phone users' privacy interests when the government seeks CSLI today. Indeed, that is one of the reasons the 2010 hearing was necessary:

> [M]obile communication devices have evolved from being little more than a convenience for the wealthy to a basic necessity for most Americans. Cell phones have transformed the way we communicate and work with each other on a daily basis... According to a 2009 Wireless Association report, there were approximately 227 million cell phone services subscribers in the United States last year. That is about 90 percent of the overall population.

Id. at 3-4 (Rep. Johnson); *see also id.* at 3 (Rep. Sensenbrenner: "I think we all know that a 24-year-old original law and a 16-year-old second law is way out of date compared to where the technology is at.").

When the SCA was passed in 1986, there were only 1,000 cell sites in the United States, and fewer than 1% of Americans used cell phones.[21] When the SCA was amended in 1994, fewer than 10% of Americans used cell phones.[22] Today, more than 90% of American adults have one. The increase in the number of cell phones and the uses to which they are put has driven a corresponding increase in the number of base stations, which means CSLI is much more

---

the government seeks historical cell site records using a § 2703(d) order, it complies with this statute.").

[21] Andrea Meyer, 30th Anniversary of the First Commercial Cell Phone Call, Verizon Wireless News Center, (October 11, 2013), http://www.verizonwireless.com/news/article/2013/10/30th-anniversary-cell-phone.html.

accurate now than it was in 1986 or in 1994. 2013 ECPA Hearing at 43 (Blaze testimony). Modern technology allows a cell phone's location to be identified with accuracy close to that of GPS.[23] *Id.* at 56 (Blaze written remarks).

Federal and local law enforcement agencies have taken advantage of the proliferation of cell phones and cell networks, seeking CSLI in more than a million cases a year.[24] The government has sought CSLI almost always in secret and almost always without a warrant, as in this case. *See, e.g.*, 2010 ECPA Hearing at 77 (testimony of Magistrate Smith referring to "regime of secrecy"); Jennifer Valentino-DeVries, Sealed Court Files Obscure Rise in Electronic Serveillance, Wall Street Journal, June 2, 2014[25] (discussing indefinite sealing of most government non-warrant requests for electronic surveillance, including CSLI).

The SCA was not enacted – or amended – to address the proliferation of government requests for CSLI. Since its passage (28 years ago) and most recent amendment (20 years ago), there have been tremendous technical advances in the accuracy of location information. That, along with Americans' widespread dependence on cell phones for an ever-increasing number of

---

[22] Andrew Kupfer, AT&T's $12 Billion Cellular Dream, Fortune, Dec. 12, 1994, at 110, available at http://archive.fortune.com/magazines/fortune/fortune_archive/1994/12/12/80051/index.htm.

[23] FCC regulations require cell phone carriers to provide increasingly accurate location information. *See* 47 C.F.R. § 20.18(h) (setting standards for carriers' ability to locate phones within as little as 100 meters for "network based" calls and as little as 50 meters for "hand-set" based calls for increasingly large percentages of their networks between 2012 and 2019); *see also In re Application*, 620 F.3d at 318 (noting FCC regulation).

[24] According to responses from eight providers to an inquiry from Senator Markey, law enforcement agencies requested "personal mobile phone data" for Americans more than one million times in 2012. For Second Year in a Row, Markey Investigation Reveals more than One Million Requests by Law Enforcement for Americans Mobile Phone Data, Press Release from Ed Markey, (December 9, 2013) available at: http://www.markey.senate.gov/news/press-releases/for-second-year-in-a-row-markey-investigation-reveals-more-than-one-million-requests-by-law-enforcement-for-americans-mobile-phone-data; *see also* 2010 ECPA Hearing at 76, 80 (testimony of Magistrate Smith, estimating that "the total number of electronic surveillance orders issued at the federal level each year substantially exceeds 10,000."). As noted above, in this district alone, the government has identified 760 matters that likely involved applications for location-tracking information from 2008 through 2012.

[25] Available at http://online.wsj.com/articles/sealed-court-files-obscure-rise-in-electronic-surveillance-1401761770.

professional and personal activities and the government's relentless pursuit of location information, requires at least a new assessment of the interests at stake in allowing the government routinely to obtain CSLI without a warrant.

V. THE SCA GIVES MAGISTRATES DISCRETION TO REQUIRE A WARRANT FOR CSLI

Even if the Fourth Amendment did not apply to CSLI, the text of the SCA gives magistrate judges discretion to require the government to establish probable cause supporting a warrant before they authorize the release of this information. *See In the Matter of the Application*, 620 F.3d at 319 ("the statute as presently written gives the [magistrate] the option to require a warrant showing probable cause."). When faced with a question of statutory interpretation, courts must rely on "[a]nalysis of the statutory text, aided by established principles of interpretation." *POM Wonderful LLC v. Coca-Cola Co.*, 132 S. Ct. 2228, 2236 (2014). "'If the plain meaning of the statute is unambiguous, that meaning is controlling.'" *United States v. Johnson*, 680 F.3d 1140, 1144 (9th Cir. 2012) (quoting *United States v. Williams*, 659 F.3d 1223, 1225 (9th Cir. 2011) (ellipses omitted)). Only if the statutory language is ambiguous does a court need to resort to legislative history. *Williams*, 659 F.3d at 1225; *see also Reeb v. Thomas*, 636 F.3d 1224, 1226-67 (9th Cir. 2011) ("When the words of a statute are unambiguous judicial inquiry is complete." (internal quotation marks omitted)).

The SCA sets forth procedures by which the government can obtain both content and subscriber information from a cell phone service provider. 18 U.S.C. § 2703(a), (b), (c). The government generally may obtain non-content information without the customer's consent "only when the governmental entity – (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure…; [or] (B) obtains a court order for such disclosure under subsection (d) of this section." 18 U.S.C. § 2703(c).

Subsection (d) states,

> [a] court order for disclosure under subsection (b) or (c) *may be issued* by any court that is a court of competent jurisdiction and *shall issue only if* the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

18 U.S.C. § 2703(d) (emphases added). "May be issued" is "the language of permission, rather than mandate." *In the Matter of the Application*, 620 F.3d at 315. Accordingly, the Third Circuit held, the plain language of § 2703 gives magistrates the discretion to require the government to show probable cause supporting a warrant to obtain CSLI.[26] *See id.* at 319 ("If Congress wished that courts 'shall,' rather than 'may,' issue § 2703(d) orders whenever the intermediate standard is met, Congress could easily have said so.").

"At the very least, the use of 'may issue' strongly implies court discretion, an implication bolstered by the subsequent use of the phrase 'only if' in the same sentence." *Id.* at 315. The phrase "only if" indicates that the showing is "a *necessary*, but not a *sufficient*, condition" for issuance of the order. *See California v. Hodari D.*, 499 U.S. 621, 628 (1991) (analyzing phrase in contest of the *Mendenhall* test for determining whether a person has been seized; emphases in original). In other words, § 2703(d) does not require the magistrate to issue the CSLI disclosure order even if the government makes the required showing. S*ee In re Application*, 724 F.3d at 619 (Dennis, J., dissenting) ("The best plain reading of this language is simply that an order *may not issue unless* the standard is met… nowhere does the statute by its terms *require* a court to

[26]As the Third Circuit recognized, even with discretion, magistrates could not act arbitrarily. *In re Application*, 620 F.3d at 316-17. "Discretion is not whim…" *Martin v. Franklin Capital Corp.*, 546 U.S. 132, 139 (2005). A court must have a reason to support its use of discretion, and that reason cannot be based on an error of law or fact. *See United States v. Ressam*, 679 F.3d 1069, 1086 (9th Cir. 2012) (en banc) ("a district court abuses its discretion when it makes an error of law, when it rests its decision on clearly erroneous findings of fact, or when we are left with a definite and firm conviction that the district court committed a clear error of judgment." (internal quotation marks and brackets omitted)).

issue a § 2703(d) order *whenever* the government's application demonstrates reasonable suspicion.") (emphases in original; footnote omitted)).

Reading § 2703(d)'s "shall" as a command rather than a permission would render "only" surplusage: "[T]he difference between 'shall… if'… and 'shall … *only* if'… is dispositive." *In the Matter of the Application*, 620 F.3d at 315. As the Third Circuit stated, "the statute does contain the word 'only' and neither we nor the Government is free to rewrite it." *Id.* at 316; *see also Beck v. Prupis*, 529 U.S. 494, 506 (2000) (referring to "the longstanding canon of statutory construction that terms in a statute should not be construed so as to render any provision of that statute meaningless or superfluous.").

For the "only" in § 2703(d) to have meaning, it must be construed to allow a magistrate the discretion to deny an application for an order under § 2703(d) even if the government has made the necessary showing. To read the statute otherwise, the Third Circuit noted, "could give the Government the virtually unreviewable authority to demand a § 2703(d) order on nothing more than its assertion. Nothing in the legislative history suggests that this was a result Congress contemplated." *In the Matter of the Application*, 620 F.3d at 317. Denying magistrates discretion to decline to issue § 2703(d) orders "would preclude magistrate judges from inquiring into the types of information that would actually be disclosed by a cell phone provider in response to the Government's request, or from making a judgment about the possibility that such disclosure would implicate the Fourth Amendment, as it could if it would disclose location information about the interior of a home."[27] *Id.*

[27] Section 2703(d)'s plain meaning is made all the clearer by comparison to the pen register statute's mandatory language, where there is no "only," and the court simply "shall issue [an order for pen register surveillance] if" the government makes the required certification. 18 U.S.C. § 3123(a)(1); *see also* Fed. R. Crim. P. 41(d)(1) (providing, in mandatory terms, that judge "must issue the warrant if there is probable cause" for search or seizure).

Moreover, the statute explicitly encompasses the possibility that the government would obtain a warrant, supported by probable cause, to obtain non-content information, such as CSLI, from cell phone providers. *See* 18 U.S.C. § 2703(c)(1)(A) (authorizing government to obtain non-content records or information with federal or state warrant). "[I]f magistrate judges were required to provide orders under § 2703(d), then the Government would never be required to make the higher showing required to obtain a warrant under § 2703(c)(1)(A)." *In the Matter of the Application*, 620 F.3d at 316. The Third Circuit correctly rejected the government's argument "that obtaining a warrant to get CSLI is a purely discretionary decision to be made by it, and one that it would make only if a warrant were, in the Government's view, constitutionally required"; "it trivializes the statutory options to read the [warrant] option as included so that the Government may proceed on one paper rather than two." *Id.*

The doctrine of constitutional avoidance offers an additional reason for the Court to hold that magistrates have discretion under the SCA to require the government to obtain a warrant for CSLI. The doctrine "rest[s] on the reasonable presumption that Congress did not intend" any meaning of a statute "which raises serious constitutional doubts," *Clark v. Martinez*, 543 U.S. 371, 381 (2005), and "[i]t is therefore incumbent upon [the Court] to read the statute to eliminate those doubts so long as such a reading is not plainly contrary to the intent of Congress." *United States v. X-Citement Videos, Inc.*, 513 U.S. 64, 78 (1994); *see also Clark*, 543 U.S. at 384 (courts must adopt any "plausible" construction that would avoid serious constitutional concern). There is no indication that Congress intended to deny magistrates the discretion to reject applications for CSLI orders. *In the Matter of the Application*, 620 F.3d at 319. Allowing them the discretion to require the government to show probable cause when there is a risk of infringement upon Fourth Amendment rights does no disrespect to Congress, which explicitly provided for warrants under § 2703(d), and avoids the potential for constitutional violations.

VI. THE GOVERNMENT MAY OBTAIN CSLI WITH A WARRANT BASED ON PROBABLE CAUSE

The Federal Public Defender's position is not that the government may never obtain CSLI, only that it must seek it pursuant to a warrant supported by probable cause. When there are doubts about the constitutionality of a particular type of search, law enforcement officers should err on the side of the Fourth Amendment and get a warrant. *United States v. Johnson*, 457 U.S. 537, 560-61 (1982). Officers already seek court orders under § 2703(d) to obtain CSLI; there will rarely, if ever, be such an urgent need for this information that officers would not have time to get a warrant. *See Riley*, 134 S. Ct. at 2493 ("Recent technological advances…have… made the process of obtaining a warrant itself more efficient."); Fed. R. Crim. P. 41(d)(3) (authorizing magistrates to issue warrant based on information communicated by phone "or other reliable electronic means").

In holding that the Fourth Amendment generally requires police to get a warrant before searching a cell phone seized incident to arrest, the Supreme Court acknowledged that its decision would "have an impact on the ability of law enforcement to combat crime" and that cell phones "can provide valuable incriminating information about dangerous criminals." *Riley*, 134 S. Ct. at 2493. The same is true of CSLI. But in striking the balance between a user's right to privacy in "all [cell phones] contain and all they may reveal," *id.* at 2494, and law enforcement's interest in obtaining this information, the Court chose to protect privacy: "Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple — get a warrant." *Id.* at 2495. "Get a warrant" should be the Court's response when the government seeks cell site location information as well.

CONCLUSION

In *Jones* and *Riley*, the Supreme Court confirmed that the Fourth Amendment continues – and changes – to protect reasonable expectations of privacy in a digital age. We all have a reasonable expectation of privacy in our movements over time in public and, especially, private spaces. Cell phone users reasonably expect that the government will not use their cell phones to track and record their movements, at least without adequate and constitutional justification. This Court should follow the Eleventh Circuit in requiring the government to obtain a warrant when it seeks CSLI.

Dated: July 28, 2014

Respectfully submitted,

STEVEN G. KALAR
Federal Public Defender

/S/ Ellen V. Leonida
ELLEN V. LEONIDA
Assistant Federal Public Defender